Assignment # *A5_P1* (*Computer Security and Privacy*) [Mahavir Jhawar]
Submission Deadline: May 2, 2018
Marks: 29

This assignment requires you to implement an SSL client-server system. The system must work as follows:

- SetUp:
  - Consider the following two entities: a certifying authority "A" and a server "S".
  - Use OpenSSL to create a signing key pair (choose any digital signature supported by SSL) $(\mathsf{pk}_A, \mathsf{sk}_A)$ for A, and a public key encryption pair $(\mathsf{pk}_S, \mathsf{sk}_S)$ for server S.
  - Generate, using OpenSSL, a self signed certificate $(\mathsf{cert}_{A\to A})$ for A binding the public key pk_A to A's identity.
  - Make A issue, using OpenSSL, a certificate to S $(\mathsf{cert}_{A\to S})$ - binding pk_S to S's identity .
- Client-Server Communication:
  - The server will start (say at host with ip address a.b.c.d and port number 3001) in passive mode listening for a transmission from the client.
  - The client will initiate an SSL connection (at a host with ip address different from a.b.c.d) to contact the server (at a.b.c.d and port 3001).
    - As part of the SSL connection, the server S must send back both the certificates $\mathsf{cert}_{A\to A}$ and $\mathsf{cert}_{A\to S}$.
    - The client must be equipped with the public key pk_A of A to verify both these certificates.
  - Upon acceptance of the SSL connection, the client will pass two integers to the server.
  - On receiving the integers, the server should add both the integers and send the result back to client.
  - The client will display the result and exit.